

1 David S. Casey, Jr. (SBN 060768)

2 *dcasey@cglaw.com*

3 Gayle M. Blatt (SBN 122048)

4 *gmb@cglaw.com*

5 Jeremy Robinson (SBN 188325)

6 *jrobinson@cglaw.com*

7 **Casey Gerry Schenk**

8 **Francavilla Blatt & Penfield, LLP**

9 110 Laurel Street

10 San Diego, California 92101

11 (619) 238-1811 phone

12 (619) 544-9232 fax

13 Attorneys for Plaintiff

14 **United States District Court**

15 **Northern District of California**

16 **Oakland Division**

17 **JASPER SCHMIDT**, on behalf of himself
18 and all others similarly situated,

19 Plaintiff,

20 v.

21 **FACEBOOK Inc.**, a Delaware Corporation,

22 Defendant.

Case No.

Class Action Complaint for Damages

Demand for Jury Trial

SUMMARY

1. Facebook operates the world’s largest social media platform with over two billion users.¹ Facebook requires that its users, including Plaintiff and the class members, give Facebook their personally identifiable information (“PII”) to use the website. Facebook collects thousands of PII data points including: users’ names, email address, telephone numbers, dates of birth, credit card numbers, private messages, locations, education and work history, and photographs. Users expect that Facebook will protect and keep their personal information secure, because Facebook explicitly says it will do just that.

2. However, over the course of the last year it has been revealed that Facebook has failed its users multiple times and has allowed unimpeded access to their accounts. Facebook first allowed a third-party company to access millions of users’ PII.² Then Facebook allowed that company to use its advertising tools to target advertisements at users’ based on their stolen information.³ Facebook did not investigate this breach and did not provide notice to users until a whistleblower revealed the breach to the Guardian.⁴

3. Facebook’s blasé attitude towards users’ PII has continued, and Facebook revealed on September 28, 2018 that its inadequate security resulted in a data breach that potentially affected over 50 million users.⁵ The breach allowed hackers to effectively take over a user’s account and steal all the information – including PII – they had put on the site. Facebook first learned of an unusual spike of activity on September 14, 2018, but did not notify users for fourteen days. The vulnerability in Facebook’s code that attackers exploited

¹ Global social media ranking 2018 | Statistic, Statista (2018), <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (last visited Oct 10, 2018).

² Emma Graham-Harrison & Carole Cadwalladr, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach The Guardian (2018), <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (last visited Oct 10, 2018).

³ *Id.*

⁴ *Id.*

⁵ “Security Update”, Facebook Newsroom (2018), <https://newsroom.fb.com/news/2018/09/security-update/> (last visited Oct 10, 2018).

1 has existed since 2017, and Facebook does not currently know how long hackers had access
2 to accounts. Instead of immediately informing users that their accounts may have been
3 hacked, Facebook decided to just log users out of their accounts without telling them why
4 it was happening. Facebook has admitted that “attackers exploited a vulnerability in
5 Facebook’s code that impacted ‘view as,’ a feature that lets people see what their own
6 profile looks like to someone else. This allowed them to steal Facebook access tokens which
7 they could then use to take over people’s accounts.”⁶ Access tokens are equivalent to a
8 digital key that allowed users to stay logged in to Facebook so that they do not need to re-
9 enter their password every time they used Facebook.⁷

10 4. On October 12th, 2018, Facebook provided further details of the breach and
11 claimed that of the original 50 million people whose access tokens Facebook thought was
12 affected, about 30 million actually had their tokens stolen.⁸

13 5. Because of Facebook’s inadequate security measures and its unreasonable
14 delay in notifying users of the breach, Plaintiff’s and class members’ PII has been
15 compromised. Plaintiff and class members have suffered harm in that their PII has lost
16 value and they must now undertake additional security measures to minimize the risk of
17 identity theft. Even with that, Plaintiff and the class members have no way to completely
18 mitigate the effects of this data breach as hackers had access to photographs and private
19 messages that now can never be removed from the internet.

20 THE PARTIES

21 6. Plaintiff Jasper Schmidt is a resident of Jenner, California. Plaintiff has had a
22 Facebook account since 2008. Plaintiff has kept his security setting at the most secured
23 allowed by Facebook, including two factor authentications. On September 28, 2018,
24 Plaintiff received a notification from Facebook that Plaintiff’s account and PII was

25
26 ⁶ “Security Update,” Facebook Newsroom (2018), [https://newsroom.fb.com/news/2018/09/security-](https://newsroom.fb.com/news/2018/09/security-update/)
update/ (last visited Oct 10, 2018).

27 ⁷ *Id.*

28 ⁸ “An Update on the Security Issue,” Facebook Newsroom (2018), [https://newsroom.fb.com/news/2018-10-](https://newsroom.fb.com/news/2018-10-update-on-security-issue/)
update-on-security-issue/ (last visited October 15, 2018)

1 compromised. Facebook has further notified Plaintiff that “attackers accessed...name,
2 primary email, most recent phone number, username, date of birth, gender, types of
3 devices you’ve used to access Facebook, relationship status, religion, hometown, current
4 city, work, 15 most recent searches on Facebook, photos.”

5 7. Defendant Facebook, Inc., is a Delaware corporation with its principal
6 executive offices located at 1601 Willow Road, Menlo Park, California 94025.

7 **JURISDICTION AND VENUE**

8 8. Subject matter jurisdiction in this civil action is authorized pursuant to 28
9 U.S.C. § 1332(d) because there are more than one hundred Class members, a majority of
10 Class Members are citizens of states that are diverse from Facebook, and the amount in
11 controversy exceeds \$5 million, exclusive of interest and costs.

12 9. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) because
13 Facebook has established sufficient contacts in this district such that personal jurisdiction is
14 appropriate. Facebook is deemed to reside in this district pursuant to 28 U.S.C. § 1391(a)

15 10. Facebook is headquartered in Menlo Park, California has conducted business
16 in this district and has availed itself of California’s markets through its marketing and
17 operations of its social networking websites and mobile applications. Venue is proper in
18 this Court pursuant to 28 U.S.C. §1391(a). In addition, Facebook’s Terms of Service contain
19 a venue clause that states: “For any claim, cause of action, or dispute you have against us
20 that arises out of or relates to these Terms or the Facebook Products ("claim"), you agree
21 that it will be resolved exclusively in the U.S. District Court for the Northern District of
22 California or a state court located in San Mateo County. You also agree to submit to the
23 personal jurisdiction of either of these courts for the purpose of litigating any such claim,
24 and that the laws of the State of California will govern these Terms and any claim, without
25 regard to conflict of law provisions.”⁹

26
27
28 ⁹ Facebook Terms of Service, <https://www.facebook.com/terms.php> (Last visited 11/15/18).

INTRADISTRICT ASSIGNMENT

11. Pursuant to Northern District of California Local Rule 3-2(c) and 3-2(d), assignment to the Oakland Division of this District is proper because a substantial part of the events or omissions giving rise to Plaintiff's and the proposed Class's claims originated from Facebook's headquarters, located in one of the counties served by the Oakland Division.

FACTUAL ALLEGATIONS

12. Facebook was founded in 2004 by Mark Zuckerberg while a student at Harvard College. Since 2006, Facebook has been open to all users over the age of thirteen with an email address.¹⁰ As of June 30, 2018, Facebook had 2.23 billion monthly active users around the world.¹¹

13. Plaintiff and Class members signed up for Facebook accounts that included providing personally identifiable information.

14. Facebook's terms of service provide comfort to their users about the security of their personal data: "People will only build community on Facebook if they feel safe. We employ dedicated teams around the world and develop advanced technical systems to detect misuse of our Products..."¹²

15. "Facebook's Privacy Principles" reinforce this sense of security to its users. "We work around the clock to help protect people's accounts, and we build security into every Facebook product. Our security systems run millions of times per second to help catch threats automatically and remove them before they ever reach you. You can also use our security tools like two-factor authentication to help keep your account even more secure."¹³

¹⁰ "47 Incredible Facebook Statistics and Facts," <https://www.brandwatch.com/blog/47-facebook-statistics/> (last visited October 16, 2018)

¹¹ "Facebook Fast Facts," <https://www.cnn.com/2014/02/11/world/facebook-fast-facts/index.html> (last visited October 16, 2018)

¹² Facebook Terms of Service, <https://facebook.com/terms.php> (last visited October 15, 2018)

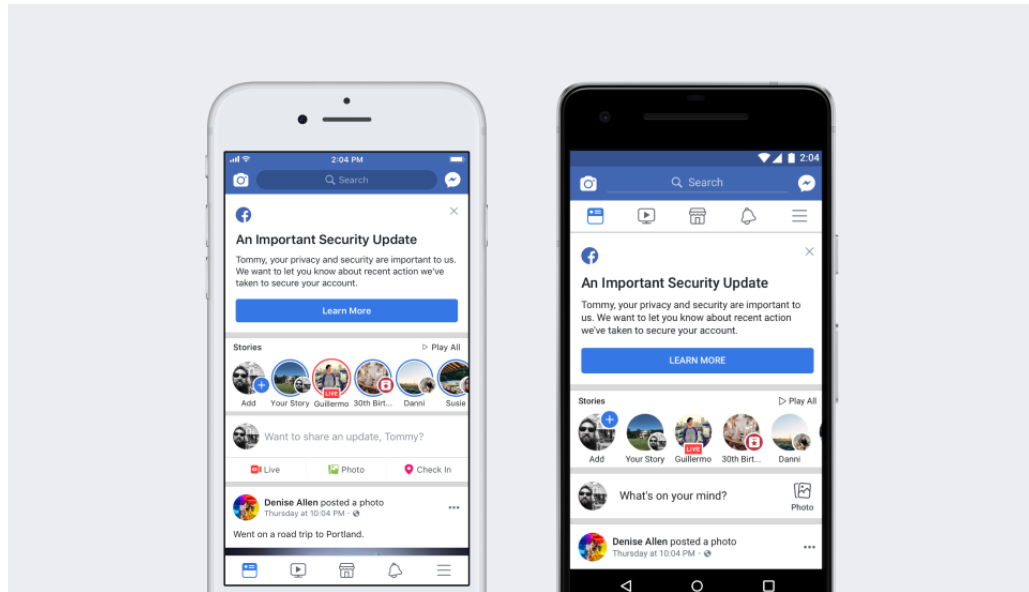
¹³ Facebook's Privacy Principles, <https://www.facebook.com/about/basics/privacy-principles> (last visited October 15, 2018)

1 16. Earlier this year, that trust was broken when news broke of the Cambridge
2 Analytica scandal involving Facebook user's personal data.¹⁴

3 17. That trust was again broken on September 28, 2018 when Facebook
4 announced a "security issue affecting almost 50 million accounts."¹⁵

5 18. According to Facebook's initial announcement of this breach, "attackers
6 exploited a vulnerability in Facebook's code that impacted the 'View As' feature that lets
7 people see what their own profile looks like to someone else. This allowed them to steal
8 Facebook access tokens which they could then use to take over people's accounts. Access
9 tokens are the equivalent of digital keys that keep people logged in to Facebook so they
10 don't need to re-enter their password every time they use the app."¹⁶

11 19. Facebook's engineering team claims that they first learned of the "security
12 issue" on the afternoon of September 25, 2018 and publicly announced it on September 28th.
13 Later reports indicated that a usual spike of activity began on September 14th which started
14



25 ¹⁴ Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal,"
26 [https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-](https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html)
scandal.html (last visited October 16, 2018)

27 ¹⁵ "Security Update," Facebook Newsroom (2018), [https://newsroom.fb.com/news/2018/09/security-](https://newsroom.fb.com/news/2018/09/security-update/)
update/ (last visited Oct 10, 2018).

28 ¹⁶ *Id.*

1 the investigation.¹⁷

2 20. In response to the breach, Facebook reset the access tokens of the
3 approximately 50 million accounts that they believed at the time were affected. Below is an
4 image of the notification that users received.¹⁸

5 21. The breach occurred due to a combination of three bugs in Facebook's
6 systems – “when using the View As feature to view your profile as a friend, the code did
7 not remove the composer that lets people wish you a happy birthday; the video uploader
8 would generate an access token when it shouldn't have; and when the access token was
9 generated, it was not for you but the person being looked up. That access token was then
10 available in the HTML of the page, which the attackers were able to extract and exploit to
11 log in as another user.” This combination of bugs began in July 2017 when Facebook made
12 a change to their video uploading feature.¹⁹

13 22. Further harm was done when the attackers were able to take that access token
14 to other accounts, using the same actions and gaining more access tokens.

15 23. The access tokens could have also been used by the attackers to gain access to
16 user accounts with third-party companies that use the Facebook login feature. There are
17 thousands of websites that allow their users to login using their Facebook credentials as a
18 quicker way to access their site. For this reason, the full scope of the breach may not yet be
19 known.

20 24. On October 12th, Facebook provided additional details about the breach.
21 Facebook now contends that 30 million users, not 50 million, actually had their tokens
22 stolen. Facebook reported that the attackers initially gained control over a set of accounts,
23 which were connected to Facebook friends. They moved between accounts stealing access
24 tokens of those friends and then friends of those friends, totaling approximately 400,000
25 users. This method allowed the attackers to mirror what these 400,000 users would have

26
27 ¹⁷ *Id.*

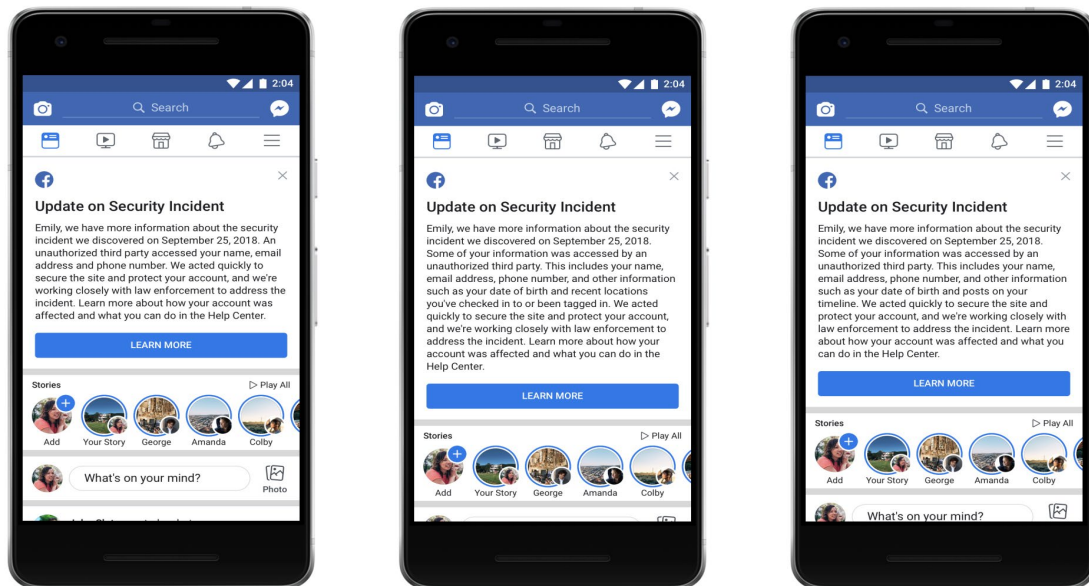
28 ¹⁸ *Id.*

¹⁹ *Id.*

seen when looking at their own profiles. The information the attackers would have seen includes: “posts on their timelines, their lists of friends, Groups they are members of, and the names of recent Messenger conversations.”²⁰

25. The attackers used this data gathered to then gain control of access tokens of about 30 million users. Facebook users in this group obtained name and contact details (phone number, email, or both, depending on what users had in their profiles). For about 14 million users in this group, the attackers had access to that information, as well as “username, gender, locale/language, relationship status, religion, hometown, self-reported current city, birthdate, device types used to access Facebook, education, work, the last 10 places they checked into or were tagged in, website, people or Pages they follow, and the 15 most recent searches.” According to Facebook, hypothetically the hackers would have been able to view the last four digits of users’ credit card numbers, but they don’t have evidence that this information was stolen.²¹

26. The identified 30 million users affected may receive customized messages from Facebook indicating what information the attackers may have accessed.



²⁰ “An Update on the Security Issue,” Facebook Newsroom (2018), <https://newsroom.fb/news/2018-10-update-on-security-issue/> (last visited October 15, 2018)

²¹ *Id.*

1 27. In addition to compromising existing accounts, the class members' PII can be
2 used by identity thieves to open new financial accounts, incur charges in the name of Class
3 members, take out loans, clone credit and debit cards, and other unauthorized activities.

4 28. Identity thieves can also use the PII to harm the Class members in a variety of
5 way, including online harassment or embarrassment, or to commit different types of fraud.
6 A Presidential Report on identity theft from 2008 states that:

7 In addition to the losses that result when identity thieves fraudulently open
8 accounts or misuse existing accounts, . . . individual victims often suffer
9 indirect financial costs, including the costs incurred in both civil litigation
10 initiated by creditors and in overcoming the many obstacles they face in
11 obtaining or retaining credit. Victims of non-financial identity theft, for
example, health-related or criminal record fraud, face other types of harm and
frustration.

12 In addition to out-of-pocket expenses that can reach thousands of dollars for
13 the victims of new account identity theft, and the emotional toll identity theft
14 can take, some victims have to spend what can be a considerable amount of
15 time to repair the damage caused by the identity thieves. Victims of new
16 account identity theft, for example, must correct fraudulent information in
17 their credit reports and monitor their reports for future inaccuracies, close
existing bank accounts and open new ones, and dispute charges with
individual creditors.

18 The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic*
19 *Plan*, at p.11 (April 2007), available at
20 [http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-](http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf)
[strategic-plan/strategicplan.pdf](http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf).

21 29. To emphasize the large-scale impact of cybercrime, a study released in
22 February 2018 by McAfee and think tank the Center for Strategic and International Studies
23 that shows worldwide cybercrime costs an estimated \$600 billion USD a year. This
24 increased from \$500 billion USD in 2014. The new estimate amounts to 0.8 percent of
25 global gross domestic product.²²

26
27
28 ²² "The Cost of Cybercrime," <https://internetsociety.org/blog/2018/02/the-cost-of-cybercrime/> (last visited on October 16, 2018)

1 30. Plaintiff and Class members are at risk for identity theft in its myriad forms,
2 potentially for the remainder of their lives

3 31. The types of information compromised in this data breach are highly valuable
4 to identity thieves. In addition to credit and debit card information, names, email
5 addresses, recovery email accounts, telephone numbers, birthdates, passwords and
6 security question answers can all be used to gain access to a variety of existing accounts
7 and websites.

8 32. Identity thieves can also use the PII to harm Plaintiffs and Class members
9 through embarrassment, blackmail, or harassment in person or online, or to commit other
10 types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax
11 returns and refunds, and obtaining government benefits.

12 33. In addition to the losses that result when identity thieves fraudulently open
13 accounts or misuse existing accounts, . . . individual victims often suffer indirect financial
14 costs, including the costs incurred in both civil litigation initiated by creditors and in
15 overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-
16 financial identity theft, for example, health-related or criminal record fraud, face other
17 types of harm and frustration.

18 34. In addition to out-of-pocket expenses that can reach thousands of dollars for
19 the victims of new account identity theft, and the emotional toll identity theft can take,
20 some victims have to spend what can be a considerable amount of time to repair the
21 damage caused by the identity thieves. Victims of new account identity theft, for example,
22 must correct fraudulent information in their credit reports and monitor their reports for
23 future inaccuracies, close existing bank accounts and open new ones, and dispute charges
24 with individual creditors.

25 35. The problems associated with identity theft are exacerbated by the fact that
26 many identity thieves will wait years before attempting to use the PII they have obtained.
27 Indeed, to protect themselves, Class members will need to remain vigilant against
28 unauthorized data use for years and decades to come.

1 36. Once stolen, PII can be used in several different ways. One of the most
2 common is that it is offered for sale on the “dark web,” a heavily encrypted part of the
3 Internet that makes it difficult for authorities to detect the location or owners of a website.
4 The dark web is not indexed by normal search engines such as Google and is only
5 accessible using a Tor browser (or similar tool), which aims to conceal users’ identities and
6 online activity. The dark web is notorious for hosting marketplaces selling illegal items
7 such as weapons, drugs, and PII. Websites appear and disappear quickly, making it a very
8 dynamic environment.

9 37. Once someone buys PII, it is then used to gain access to different areas of the
10 victim’s digital life, including bank accounts, social media, and credit card details. During
11 that process, other sensitive data may be harvested from the victim’s accounts, as well as
12 from those belonging to family, friends, and colleagues.

13 38. Further, an individual’s PII has market value and there are markets for that
14 PII. For example, data collection companies, credit reporting companies, and companies
15 that engage in targeted advertising are all willing to pay money to obtain, directly or
16 indirectly, PII from individuals. Indeed, many email and social media service providers
17 require their users to consent to having their information scanned and recorded for the
18 purpose of selling that information to advertisers. But, the theft of that PII and
19 unauthorized sale of it on the “dark web” diminishes its legitimate market value.

20 39. In fact, hackers are already selling Facebook logins for \$2.60 each on the dark
21 web, according to a study by Money Guru released within days of the latest breach.²³

22 40. Facebook users whose PII has been unlawfully accessed or stolen can – and
23 should – sign up for credit protection services immediately. Such services cost money,
24 however. For example, according to the California Department of Justice, the three main
25 credit bureaus each charge \$10 to “freeze” credit files. <https://oag.ca.gov/idthemf/facts/freeze->

26
27
28 ²³ “Hackers Selling Facebook Logins on the Dark Web for \$2,” <http://nypost.com/2018/10/01/hackers-are-selling-facebook-logins-on-the-dark-web-for-2/> (last visited October 16, 2018)

1 *your-credit*. Facebook has yet to offer to reimburse such costs for the millions of users
2 affected by the breach.

3 CLASS ACTION ALLEGATIONS

4 41. Plaintiff brings this lawsuit on behalf of himself and as a class action on
5 behalf of a proposed national class, defined as:

6
7 All persons in the United States who were or are Facebook users and whose
8 personal information was accessed, compromised, or stolen from Facebook in
the data breach that was announced on September 28, 2018.

9
10 42. Plaintiff also brings this lawsuit on behalf of himself and as a California
11 subclass, defined as:

12 All persons in the State of California who were or are Facebook account
13 holders and whose personal information was accessed, compromised, or
14 stolen from Facebook in the data breach that was announced on September
28, 2018.

15 43. Collectively, the national class and California subclass will be referred to as
16 “the Class.”

17 44. Excluded from the Class are Defendants and any entities in which Defendant
18 or their subsidiaries or affiliates have a controlling interest; Defendant’s officers, agents,
19 and employees; attorneys for Plaintiff and the Class; the judicial officer to whom this action
20 is assigned and any member of the Court’s staff and immediate families; as well as claims
21 for personal injury, wrongful death, and emotional distress.

22 45. **Numerosity:** The members of the Class are so numerous that joinder of all
23 members would be impracticable. Plaintiff reasonably believes that Class members number
24 millions of people. As such, class members are so numerous that joinder of all members is
25 impractical. The names and addresses of class members are identifiable through documents
26 maintained by Facebook.

27 46. **Commonality and Predominance:** This action involves common questions of
28 law or fact, which predominate over any questions affecting individual Class members,

including:

- a. Whether Defendant engaged in the wrongful conduct alleged herein;
- b. Whether Defendant owed a legal duty to Plaintiffs and the other Class members to exercise due care in collecting, storing, and safeguarding their Personal Information;
- c. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiffs and the other class members to exercise due care in collecting, storing, and safeguarding their Personal Information;
- d. Whether Defendant's conduct violated Cal. Bus. & Prof. Code § 17200 *et seq.*;
- e. Whether Defendant's conduct violated Cal. Civ. Code § 1798.80 *et seq.*;
- f. Whether Plaintiff and the other class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and
- g. Whether Plaintiff and the other class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

47. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

48. **Typicality:** Plaintiff's claims are typical of the claims of the other Class members because, among other things, Plaintiff and the other Class members were injured through the substantially uniform misconduct by Facebook. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other class members, and there are no defenses that are unique to Plaintiff.

49. **Adequacy of Representation:** Plaintiff is an adequate representative of the class because his interests do not conflict with the interests of the other class members he seeks to represent; he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class' interests will

1 be fairly and adequately protected by Plaintiff and his counsel.

2 50. **Superiority:** A class action is superior to any other available means for the
 3 fair and efficient adjudication of this controversy, and no unusual difficulties are likely to
 4 be encountered in the management of this matter as a class action. The damages, harm, or
 5 other financial detriment suffered individually by Plaintiff and the other Class members
 6 are relatively small compared to the burden and expense that would be required to litigate
 7 his claims on an individual basis against Defendant, making it impracticable for class
 8 members to individually seek redress for Defendant's wrongful conduct. Even if class
 9 members could afford individual litigation, the court system could not. Individualized
 10 litigation would create a potential for inconsistent or contradictory judgments and increase
 11 the delay and expense to all parties and the court system. By contrast, the class action
 12 device presents far fewer management difficulties and provides the benefits of single
 13 adjudication, economies of scale, and comprehensive supervision by a single court.

14 51. **Application of California law:** Because Facebook is headquartered in
 15 California and all its key decisions and operations emanate from California, California law
 16 can and should apply to all claims relating to the data breach, even those made by persons
 17 who reside outside of California. Additionally, Facebook's Terms of Service contain a
 18 choice of law provision specifying California law as governing all aspects of the
 19 relationship between Facebook and its users.

20 **FIRST CAUSE OF ACTION**

21 **Unfair and Unlawful Business Acts and Practices**

22 **Cal. Bus. & Prof. Code § 17200, et seq.**

23 **(On behalf of the Nationwide Class and the California Class)**

24 52. Plaintiff repeats, realleges, and incorporates by reference the allegations in
 25 paragraphs 1 through 51, as though fully stated herein.

26 53. Defendant's acts and practices, as alleged in this Complaint, constitute unfair
 27
 28

1 and unlawful business practices in violation of the Unfair Competition Law (“UCL”), Cal.
2 Bus. & Prof. Code § 17200, *et seq.*

3 54. By reason of the conduct alleged herein, Facebook engaged in unlawful,
4 unfair, and deceptive practices within the meaning of the UCL. The conduct alleged herein
5 is a “business practice” within the meaning of the UCL.

6 55. Defendant stored Plaintiff’s and the other Class members’ PII in their
7 electronic and consumer information databases. Facebook represented to Plaintiff and the
8 other Class members that its PII databases were secure and that users’ PII would remain
9 private. Facebook engaged in deceptive acts and business practices by providing in its
10 website that “We work hard to keep your information secure. We work around the clock to
11 help protect people’s accounts, and we build security into every Facebook product. Our
12 security systems run millions of times per second to help catch threats automatically and
13 remove them before they ever reach you.” [https://www.facebook.com/about/basics/privacy-](https://www.facebook.com/about/basics/privacy-principles)
14 [principles](https://www.facebook.com/about/basics/privacy-principles)

15 56. Facebook knew or should have known that it did not employ reasonable
16 measures that would have kept Plaintiff’s and the other Class members’ PII secure and
17 prevented the loss or misuse of Plaintiff’s and the other Class members’ PII.

18 57. Facebook’s representations that it would secure and protect Plaintiff’s and the
19 other Class members’ PII in its possession were facts that reasonable persons could be
20 expected to rely upon when deciding whether to use Facebook’s services.

21 58. Defendant violated the Unfair and Unlawful prongs of the UCL by
22 misrepresenting the safety of their many systems and services, specifically the security
23 thereof, and their ability to safely store Plaintiff’s and Class members’ PII. Facebook also
24 violated the UCL by failing to immediately notify Plaintiff and the other Class members of
25 the data breach. If Plaintiff and the other Class members had been notified in an
26 appropriate fashion, they could have taken precautions to safeguard their PII.

27 59. Defendant’s acts, omissions, and misrepresentations as alleged herein were
28 unlawful, unfair and in violation of, *inter alia*, Cal. Bus. & Prof. Code §17500 *et seq.*, and Cal.

1 Civ. Code § 1798.80 *et seq.*

2 60. Plaintiff and the other Class members suffered injury in fact as the result of
3 Defendant's failure to secure Plaintiff's and the other Class members' PII contained in
4 Defendant's servers or databases.

5 61. As a result of Facebook's violations of the UCL, Plaintiff and the other Class
6 members are entitled to restitution and injunctive relief.

7 **SECOND CAUSE OF ACTION**

8 **Violation of the California Customer Records Act**

9 **Cal. Civ. Code § 1798.80, *et seq.***

10 **(On behalf of the California Class)**

11 62. Plaintiff realleges and incorporates by reference the allegations in paragraphs
12 1 through 51 as if fully set forth herein.

13 63. Plaintiff brings this cause of action on behalf of the California Class whose
14 personal user information is maintained by Facebook and which was compromised.

15 64. "[T]o ensure that personal information about California residents is
16 protected," the California Legislature enacted Civil Code § 1798.81.5, which requires that
17 any business that "owns, licenses, or maintains personal information about a California
18 resident shall implement and maintain reasonable security procedures and practices
19 appropriate to the nature of the information, to protect the personal information from
20 unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code §
21 1798.81.5(b).

22 65. Facebook is a "business" within the meaning of Civil Code § 1798.80(a).

23 66. Plaintiff and members of the Class are "individual[s]" within the meaning of
24 the Civil Code § 1798.80(d). Pursuant to Civil Code § 1798.80(e), the user information is
25 "personal information," which includes, but is not limited to, an individual's name,
26 physical characteristics or description, address, telephone number, education, employment,
27 employment history, and medical information.

28 67. The breach of the personal information of tens of millions of Facebook users

1 constituted a “breach of the security system” of Facebook pursuant to Civil Code §
2 1798.82(g).

3 68. By failing to implement reasonable measures to protect its users’ information,
4 Facebook violated Civil Code § 1798.81.5.

5 69. As alleged above, Facebook unreasonably delayed informing anyone about
6 the breach of security of Plaintiff’s and other Class members’ confidential and non-public
7 PII after Defendant knew the breach had occurred.

8 70. Facebook failed to disclose to Plaintiff and other Class members, without
9 unreasonable delay, and in the most expedient time possible, the breach of security of their
10 unencrypted, or not properly and securely encrypted, and when they knew or reasonably
11 believed such information had been compromised.

12 71. Facebook’s ongoing business interests, and in particular the earlier scandals
13 involving Cambridge Analytica and reports of fake accounts and news around the 2016
14 election, gave Facebook incentive to want to conceal the breach from the public.

15 72. Upon information and belief, no law enforcement agency instructed Facebook
16 that notification to Plaintiff or other Class members would impede its investigation.

17 73. Accordingly, Plaintiff requests that the Court enter an injunction requiring
18 Facebook to implement and maintain reasonable security procedures to protect its users’
19 personal information in compliance with the California Customer Records Act. Plaintiff
20 requests that the Court require Facebook to identify and notify all members of the Class
21 who have not yet been informed of the breach.

22 74. As a result of Facebook’s violations of California Civil Code §§ 1798.81.5 and
23 1798.82, Plaintiff and members of the Class have and will incur economic damages relating
24 to time and money spend remedying the breach, such as monitoring their online presence
25 to ensure that their identity has not been stolen or coopted for an illicit purpose.

26 75. Plaintiff, for himself and on behalf of the members of the Class, seek all
27 remedies available under California Civil Code § 1798.84, including, but not limited to
28 damages suffered by members of the Class and equitable relief.

76. Plaintiff, for himself and on behalf of the members of the Class, also seeks reasonable attorneys' fees and costs under applicable law including California Code of Civil Procedure §1021.5 and Federal Rule of Civil Procedure 23.

THIRD CAUSE OF ACTION

Negligence

(On behalf of the Nationwide Class and California Subclass)

77. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 51, as though fully stated herein.

78. Facebook owed a duty to Plaintiff and the other Class members to exercise reasonable care in safeguarding and protecting their PII that was in its possession from being compromised, lost, stolen, misused, or disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure that Plaintiff's and the other Class members' PII was adequately secured and protected. Defendant further had a duty to implement processes that would detect a breach of their security system in a timely manner.

79. Facebook also had a duty to timely disclose to Plaintiff and the other Class members that their PII had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiff and the other Class members could take appropriate measures to cancel or change usernames, pin numbers, and passwords on compromised accounts, to begin monitoring their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts and take any and all other appropriate precautions.

80. By being entrusted by Plaintiffs and the Class to safeguard their PII, Defendant had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class signed up for Defendant's services and agreed to provide their PII with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiffs and the Class of any breaches or other security concerns that might call for action by Plaintiffs and the Class. But, Defendant did not. Defendant not only knew their data

1 security was inadequate, they also knew they didn't even have the tools to detect and
2 document intrusions or exfiltration of PII. Defendant are morally culpable, given their
3 repeated security breaches, wholly inadequate safeguards, and refusal to notify Plaintiffs
4 and the Class of breaches or security vulnerabilities.

5 81. Facebook breached its duty to exercise reasonable care in safeguarding and
6 protecting Plaintiff's and the other Class members' PII by failing to adopt, implement, and
7 maintain adequate security measures to safeguard that information; allowing unauthorized
8 access to Plaintiff's and the other Class members' PII stored by Defendant; and failing to
9 recognize in a timely manner the breach.

10 82. Facebook breached its duty to timely disclose that Plaintiff's and the other
11 Class members' PII had been, or was reasonably believed to have been, stolen or
12 compromised.

13 83. Facebook's failure to comply with industry regulations and the delay
14 between the first vulnerability date and the date Facebook informed users of the data
15 breach further evidence Facebook's negligence in failing to exercise reasonable care in
16 safeguarding and protecting Plaintiff's and the other Class members' PII.

17 84. But for Defendant's wrongful and negligent breach of its duties owed to
18 Plaintiff and the other Class members, their PII would not have been compromised, stolen,
19 and viewed by unauthorized persons.

20 85. The injury and harm suffered by Plaintiff and the other Class members was
21 the reasonably foreseeable result of Defendant's failure to exercise reasonable care in
22 safeguarding and protecting Plaintiff's and the other Class members' PII. Defendant knew
23 or should have known that their systems and technologies for processing and securing
24 Plaintiff's and the other Class members' PII had security vulnerabilities.

25 86. As a result of Defendant's negligence, Plaintiff and the other Class members
26 incurred economic damages, including expenses for credit monitoring, fraudulent charges
27 on credit card or bank accounts, forged IRS returns, loss of use and value of their debit
28 and/or credit cards, and other identity theft-related damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on her own behalf and on behalf of the Class, respectfully requests that this Court enter an Order:

- (1) Certifying the proposed Class, and appointing Plaintiff as Class Representative;
- (2) Finding that Defendant's conduct was negligent, deceptive, unfair, and unlawful as alleged herein;
- (3) Enjoining Defendant from engaging in further negligent, deceptive, unfair, and unlawful business practices as alleged herein;
- (4) Awarding Plaintiff and Class members actual, compensatory, and consequential damages;
- (5) Awarding Plaintiff and Class members statutory damages and penalties, as allowed by law;
- (6) Awarding Plaintiff and Class members restitution and disgorgement;
- (7) Awarding Plaintiff and Class members pre-judgment and post-judgment interest;
- (8) Awarding Plaintiff and Class members reasonable attorneys' fees, costs, and expenses; and
- (9) Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the proposed Class, hereby demands a trial by jury as to all matters so triable.

Dated: November 15, 2018

CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP

By: /s/Gayle M. Blatt
Gayle M Blatt.
gmb@cglaw.com

Attorneys for Plaintiff